Remediating Security-Policy Compliance issues using Ansible Playbooks

Improve Compliance Status with Automated Remediations
Remediating Security-Policy Compliance issues using Ansible Playbooks

Improve Compliance Status with Automated Remediations
Abstract

Remediate issues resulting in the noncompliance of RHEL systems with adopted security policies.

Providing Feedback: If you have a suggestion to improve this documentation, or find an error, submit a Bugzilla report at http://bugzilla.redhat.com. Select the Cloud Software Services (cloud.redhat.com) product and use the Documentation component.
Table of Contents

CHAPTER 1. COMPLIANCE SERVICE REMEDIATION OVERVIEW ........................................ 3

CHAPTER 2. REMEDIATING SYSTEMS TO IMPROVE THE COMPLIANCE THRESHOLD OF A SELECTED POLICY ................................................................................................................. 4

CHAPTER 3. REMEDIATING RULES FROM MULTIPLE POLICIES TO IMPROVE THE COMPLIANCE SCORE OF A SYSTEM ............................................................................................................. 5

CHAPTER 4. REFERENCE MATERIALS .................................................................................. 6

CHAPTER 5. IMPORTANT CHANGES WITH THE 2020-04 RELEASE OF RED HAT INSIGHTS .......... 7
CHAPTER 1. COMPLIANCE SERVICE REMEDIATION OVERVIEW

The Compliance service shows the compliance status of your Red Hat Enterprise Linux (RHEL) environment with adopted OpenSCAP security policies, and identifies the individual rules affecting the compliance of your systems.

For each rule + system pairing, the Compliance service shows the steps to resolve the issue, and enables automated remediation with the creation of Ansible Playbooks.

The Compliance service enables the following approaches to remediating issues:

- RemEDIATE multiple systems to which a single policy is applied to bring a policy up to an acceptable threshold of compliance.
- RemEDIATE multiple rules, whether for one or more policies, affecting the compliance status of a single system.
CHAPTER 2. REMEDIATING SYSTEMS TO IMPROVE THE COMPLIANCE THRESHOLD OF A SELECTED POLICY

Complete the following steps to remediate systems affecting the compliance threshold of a policy:

Procedure

1. Navigate to the Compliance service > SCAP Policies page and click on a policy.

2. Click the Systems tab.

3. Check the boxes for the systems you want to remediate and click Remediate.

4. Select whether to add the remediations to an existing or new playbook and take the following action:
   a. Click Existing Playbook and select the desired playbook from the dropdown list, OR
   b. Click Create new Playbook and add a playbook name.
   c. Click Next.

5. Review the information in the summary.
   a. Scroll to the bottom of the summary and toggle Auto Reboot if available and desired.
   b. Click Create.

Verification steps

1. Select Remediations in the Red Hat Insights services menu.

2. Locate the playbook you just created and check the box next to it.

3. Download the playbook using the Download playbook link.
CHAPTER 3. REMEDIATING RULES FROM MULTIPLE POLICIES TO IMPROVE THE COMPLIANCE SCORE OF A SYSTEM

Complete the following steps to remediate rules affecting the compliance score of a system:

**Procedure**

1. Navigate to the Compliance service > Reports page and click the By System tab.
2. Click on a system.
3. Scroll down to see the list of rules impacting the system.
4. Use filters to refine the list to expose the most critical rules.
5. Check the boxes next to the rules to remediate and click Remediate.
6. Select whether to add to an existing or new playbook and take one of the following actions:
   - a. Click Existing Playbook and select the desired playbook from the dropdown list, OR
   - b. Click Create new Playbook and add a playbook name.
   - c. Click Next.
7. Review the information in the summary.
   - a. Scroll to the bottom of the summary and toggle Auto Reboot if available and desired.
   - b. Click Create.

**Verification steps**

1. Select Remediations in the Red Hat Insights services menu.
2. Locate the playbook you just created and check the box next to it.
3. Download the playbook using the Download playbook link.
CHAPTER 4. REFERENCE MATERIALS

To learn more about the Red Hat Insights service, or the other {GUIName_short}, the following resources might also be of interest:

**Documentation**

- *Assessing and Monitoring Security Policy Compliance of RHEL Systems*
- *Generating Compliance Reports*
- *Red Hat Insights Documentation*
- *Red Hat Insights Product Support page*
CHAPTER 5. IMPORTANT CHANGES WITH THE 2020-04 RELEASE OF RED HAT INSIGHTS

The 2020-04 release of Red Hat Insights includes significant changes to the application features and services.

Changes to the Red Hat Insights application

The Red Hat Insights application now includes the services that were previously bundled with the Cloud Management Services for RHEL application, and were part of the Red Hat Smart Management bundle, along with Red Hat Satellite.

The former cloud management services, plus a couple of new services, are now included in the value that Insights brings to each Red Hat Enterprise Linux (RHEL) subscription.

Insights Advisor

The tools and capabilities that constituted Red Hat Insights prior to this release are now available as the Advisor service. The rules that have always been the currency of Insights are now called Advisor Recommendations.

Insights security rules have moved

The CVE security rules that were previously curated by the Insights rules team are now included with all other Red Hat CVEs in the Vulnerability service. Security rules are high profile CVEs, some of which have been through the Customer Security Awareness Program. They are identifiable in the Vulnerability service by a security rule icon. You can also filter security rules in the Vulnerability service.

Services included with Red Hat Insights

The services included with Red Hat Insights in the 2020-04 release are:

- Advisor. Identify and fix configuration issues that can negatively impact the availability, performance, stability, and security of RHEL systems.
- Vulnerability. Assess and monitor the exposure of your RHEL environment to CVEs and security rules.
- Compliance. Assess and monitor the compliance of your RHEL systems with SCAP security policies.
- Patch. Enable consistent patch workflows for RHEL systems across the open hybrid cloud.
- Drift. Compare system configurations of a system over time, or to other systems and baselines, to identify discrepancies in your environment and perform drift analysis.
- Policies. Evaluate and react to system configuration changes in your environment.

The integrated tools that work with each of the services above are:

- Inventory. Topological inventory of RHEL systems under Red Hat Insights management
- Remediations. Repository of Ansible Playbooks that you create and manage using Red Hat Insights
- Subscription Watch. Comprehensive, product-by-product, account-level subscription reporting service across hybrid cloud deployments
Resources

- Red Hat Insights Product Support page
- Red Hat Insights Documentation
- Red Hat Insights Release Notes
- Red Hat Insights blog channel